REMARKS

Applicants respectfully request reconsideration of this application as amended. Claims 1-6, 9 and 17-20 have been amended. Claims 10-16 and 21-24 have been cancelled without prejudice. New claims 25-30 have been added. Therefore, claims 1-9, 17-20 and 25-30 are now presented for examination.

35 U.S.C. § 103 Rejection

Claims 1-3, 5-9, and 23 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas Jr. et al., U.S. Patent No. 6687375 ("Matyas") further in view of Chen, et al., U.S. Patent No. 6,182,220 ("Chen") and in further view of Hardy et al., U.S. Patent No. 6,073,242 ("Hardy").

As an initial matter, Applicants respectfully submit that Chen and Hardy do not satisfy any of the deficiencies of Matyas. For example, Matyas discloses "it is often convenient, and it will be the practice used in describing the present inventions, to refer to the PRNG as having *only one such secret seed value*" (col. 9, lines 19-34; emphasis provided). In other words, Matyas not only discloses using a single seed value, it discourages and teaches away from referring to multiple seed values (even when multiple seed values area allowed, they are referred to as "*a single composite seed value*") (col. 9, lines 19-34; emphasis provided). In light of this, and generally, Matyas does not disclose or reasonably suggest "stirring the PRNG with the local seeding information and the additional seeding information" and it further does not disclose or reasonably suggest "securely obtaining additional seeding information from one or more remote entropy servers" as recited by claim 1 (emphasis provided).

Chen, like Matyas, does not disclose or reasonably suggest "stirring the PRNG with the local seeding information and the additional seeding information" and it further does not disclose or reasonably suggest "securely obtaining additional seeding information from one or more remote entropy servers" as recited by claim 1 (emphasis provided). Further, even in the paragraph pointed out by the Examiner (see Office Action, mailed 1/19/2005, page 3, line 9 from top), nowhere does Chen uses the term "remote" (col. 1, line 66-67-col. 2, lines 1-9).

Given Chen does not satisfy any of the deficiencies of Matyas, Hardy is irrelevant. Although Hardy mentions the term "secure connection" in col. 3, it simply provides a definition of the term "secure connection" (col. 3, lines 54-67) and does not disclose or reasonably suggest securely obtaining additional seeding information from one or more remote entropy servers as recited by claim 1. Hence, Chen and Hardy adds nothing relevant to Matyas at least with regard to claim 1. Accordingly, Applicants respectfully request the withdrawal of the rejection of claim 1 and its dependent claims.

Claims 17-22 and 24 are rejected under 35 U.S.C. §103(a) as being unpatentable over Matyas further in view of Chen.

Claim 17 and new claim 25 include limitations similar to those of claim 1. Accordingly, Applicants respectfully request the withdrawal of the rejection of claim 17 and its dependent claims and submit that new claim 25 and its dependent claims are distinguished over the cited references.

Conclusion

In light of the foregoing, reconsideration and allowance of the claims is hereby earnestly requested.

Invitation for a Telephone Interview

The Examiner is requested to call the undersigned at (303) 740-1980 if there remains any issue with allowance of the case.

Request for an Extension of Time

Applicants respectfully petition for an extension of time to respond to the outstanding Office Action pursuant to 37 C.F.R. § 1.136(a) should one be necessary. Please charge our Deposit Account No. 02-2666 to cover the necessary fee under 37 C.F.R. § 1.17(a) for such an extension.
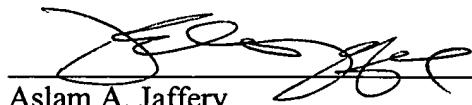
Charge our Deposit Account

Please charge any shortage to our Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN LLP

Date: March 25, 2005

Aslam A. Jaffery
Reg. No. 51,841

12400 Wilshire Boulevard
7th Floor
Los Angeles, California 90025-1030
(303) 740-1980